УДК 519.65
DOI: 10.32626/2308-5916.2019-19.75-81

П. С. Малачівський*, д-р техн. наук,
Б. Р. Монцібович*, канд. фіз.-мат. наук,
Я. В. Пізюр,** канд. фіз.-мат. наук,
Р. П. Малачівський,** інженер

*Інституту прикладних проблем механіки і математики
імені Я. С. Підстригача НАН України, м. Львів,
**Національний університет «Львівська політехніка», м. Львів

ЧЕБИШОВСЬКЕ НАБЛИЖЕННЯ РАЦІОНАЛЬНИМ ВИРАЗОМ ФУНКЦІЙ ДВОХ ЗМІННИХ

Запропоновано метод побудови чебишовського наближення раціональним виразом для функцій двох змінних. Ідея методу ґрунтується на побудові граничного середньостепеневого наближення у нормі простору L^p при $p \to \infty$. Для побудови цього наближення використано метод найменших квадратів з двома змінними ваговими функціями. Одна вагова функція забезпечує побудову середньостепеневого наближення, а друга — уточнення параметрів раціонального виразу за схемою лінеаризації. Запропоновано спосіб послідовного уточнення значень вагових функцій. Результати розв'язування тестових прикладів підтверджують ефективність використання запропонованого методу.

Ключові слова: *чебишовське наближення раціональним виразом, функції двох змінних, середньостепеневе наближення, метод найменших квадратів.*

Вступ. Нехай неперервну функцію двох змінних $f(x, y)$ задану на множині точок (x_i, y_j), $i = \overline{0, n}$, $j = \overline{0, m}$ необхідно наблизити нескорочуваним раціональним виразом

$$R_{k,l}(a,b;x,y) = \frac{\sum_{i=0}^{k} a_i \varphi_i(x,y)}{\sum_{i=0}^{l-1} b_i \varphi_i(x,y) + \varphi_l(x,y)}, \qquad (1)$$

де $\varphi_i(x,y)$, $i = \overline{0, k_m}$, $k_m = \max(k, l)$ — система базисних функцій, а a_i, $i = \overline{0, k}$ і b_i, $i = \overline{0, l-1}$ — невідомі параметри: $\{a_i\}_{i=0}^{k} \in A$, $A \subseteq R^k$, $\{b_i\}_{i=0}^{l-1} \in B$, $B \subseteq R^{l-1}$, R^m — m-вимірний векторний простір.

Побудова чебишовського наближення раціональним виразом (1) для функції $f(x, y)$ на множині точок (x_i, y_j), $i = \overline{0, n}$, $j = \overline{0, m}$ полягає в обчисленні таких значень параметрів a^* та b^*, при яких досягається виконання умови

$$\max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x, y) - R_{k,l}(a^*, b^*; x, y) \right| = \min_{a \in A,\ b \in B} \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x, y) - R_{k,l}(a, b; x, y) \right|. \quad (2)$$

На жаль, поки що немає ефективних алгоритмів для обчислення параметрів чебишовського наближення раціональним виразом [1]. Серед методів отримання чебишовського наближення функцій багатьох змінних раціональним виразом здебільшого застосовують зведення до послідовного розв'язування задачі лінійного програмування [2, 3], або метод нелінійної оптимізації [1, 4]. В працях [5, 6] описано алгоритми обчислення параметрів чебишовського наближення функцій однієї змінної на основі схеми Ремеза з використанням диференціальної корекції. Метод побудови чебишовського наближення раціональним виразом на основі обчислення середньостепеневих наближень функцій однієї змінної описано в [7].

Ми пропонуємо метод побудови чебишовського наближення функцій двох змінних раціональним виразом як граничного наближення у нормі простору L^p при $p \to \infty$. Він ґрунтується на методі описаному в [8] і полягає у послідовній побудові середньостепеневих наближень. Останні раціональним виразом обчислюються за методом найменших квадратів з використанням двох змінних вагових функцій, значення яких уточнюються з урахуванням всіх попередніх наближень. Параметри раціонального наближення за методом найменших квадратів визначаємо з використанням лінеаризації [9, 10].

1. Середньостепеневе наближення функцій раціональним виразом. Для оцінки похибки середньостепеневого наближення функції $f(x, y)$, заданої на множині точок (x_i, y_j), $i = \overline{0, n}$, $j = \overline{0, m}$, використовують норму евклідового простору E^p $(1 \le p < \infty)$

$$\|\Delta\|_{E^p} = \left(\sum_{i=0}^{n} \sum_{j=0}^{m} \left| \Delta(x_i, y_j) \right|^p \right)^{1/p}, \quad (3)$$

де $\Delta(x, y) = f(x, y) - R_{k,l}(a, b; x, y)$. Граничне значення норми $\|\Delta\|_{E^p}$ при $p \to \infty$ відповідає нормі у просторі неперервних функцій $\|\Delta\|_C$ [1].

2. Обчислення параметрів чебишовського наближення раціональним виразом. Якщо неперервне чебишовське наближення

раціональним виразом $R_{k,l}(a,b;x,y)$ (1) для функції $f(x,y)$ на множині точок (x_i, y_j), $i=\overline{0,n}$, $j=\overline{0,m}$ існує, то побудова такого наближення ґрунтується на ідеї послідовного обчислення середньостепеневих наближень при $p=2,3,4,\ldots$. Для побудови середньостепеневого наближення функції $f(x,y)$ раціональним виразом (1) в просторі E^p використовуємо метод найменших квадратів [8]

$$\sum_{i=0}^{n}\sum_{j=0}^{m}\rho_r(x_i,y_j)\left(f(x_i,y_j)-R_{k,l}(a,b;x_i,y_j)\right)^2 \xrightarrow[a\in A,\ b\in B]{} \min, \quad (4)$$

$$r=0,1,\ \ldots,p-2$$

з послідовним уточненням значень вагової функції $\rho_r(x,y)$

$$\rho_0(x,y)=1,\ \rho_r(x,y)=\prod_{i=1}^{r}\left|\Delta_i(x,y)\right|,\ r=1,\ldots,p-2,\ p=3,4,\ldots, \quad (5)$$

де $\Delta_s(x,y)=f(x,y)-R_{k,l,s-1}(a,b;x,y)$, $s=\overline{1,r}$, $R_{k,l,s}(a,b;x,y)$ — наближення за методом найменших квадратів функції $f(x,y)$ з ваговою функцією $\rho_s(x,y)$. Наближення $R_{k,l,s}(a,b;x,y)$ відповідає середньостепеневому наближенню степеня $p=s+2$.

Побудова наближення раціональним виразом за методом найменших квадратів — це нелінійна задача. Для побудови такого наближення застосовано лінеаризацію з використанням змінної вагової функції [9, 10], яка полягає в ітераційному уточненні наближення раціональним виразом (1). Відповідно до цього методу лінеаризації для кожного фіксованого значення p обчислюємо наближення функції $f(x,y)$ раціональним виразом $R_{k,l}(a,b;x,y)$ (1) за методом найменших квадратів

$$\sum_{i=0}^{n}\sum_{j=0}^{m}\rho_r(x_i,y_j)\upsilon_{r,t}(x_i,y_j)\left(\Phi_{r,t}(a,b;x_i,y_j)\right)^2 \xrightarrow[a\in A,\ b\in B]{} \min, \quad (6)$$

$$r=p-2,\ t=0,1,\ \ldots,$$

де

$$\Phi_{r,t}(a,b;x,y)=f(x,y)\left(\sum_{i=0}^{l-1}b_{i,r,t}\varphi_i(x,y)+\varphi_l(x,y)\right)-\sum_{i=0}^{k}a_{i,r,t}\varphi_i(x,y). \quad (7)$$

Значення вагової функції $\rho_r(x,y)$ обчислюємо за формулою (5), а вагової функції $\upsilon_{r,t}(x,y)$ — за формулою

$$\upsilon_{r,t}(x,y)=\begin{cases}1, \text{ якщо } & r=0,\ t=0,\\ \left(\sum_{i=0}^{l-1}b_{i,r,t-1}\varphi_i(x,y)+\varphi_l(x,y)\right)^{-2}, & \text{якщо } t>0.\end{cases} \quad (8)$$

Уточнення наближення раціональним виразом (1) за методом найменших квадратів (6), (8) можна контролювати точністю ε_1 виконання умови

$$\left| \eta_{r,t-1} - \eta_{r,t} \right| \le \varepsilon_1 \eta_{r,t}, \tag{9}$$

де

$$\eta_{r,t} = \sum_{i=0}^{n} \sum_{j=0}^{m} \rho_r(x_i, y_j) \upsilon_{r,t}(x_i, y_j) \left(\Phi_{r,t}(a,b; x_i, y_j) \right)^2 . \tag{10}$$

Під час тестування використовували значення $\varepsilon_1 = 0.003$, яке забезпечувало збіжність двох-трьох значущих цифр суми квадратів відхилень (10) на множині точок задання наближуваної функції. Виконання умови (9) означає, що середньостепеневе наближення степеня $p = r + 2$ раціональним виразом $R_{k,l,r}(a,b; x, y)$ обчислено з точністю ε_1. Значення параметрів наближення $R_{k,l,r}(a,b; x, y)$ такі:

$$a_{j,r} = a_{j,r,t} \quad (j = \overline{0, k}) \text{, а } b_{j,r} = b_{j,r,t} \quad (j = \overline{0, l-1}) . \tag{11}$$

Отже, побудова чебишовського наближення раціональним виразом (1) полягає у застосуванні двох ітераційних процесів: вкладених ітерацій (6)–(8) і зовнішніх (4), (5). Завершення ітерацій (4), (5) можна контролювати досягненням деякої заданої точності ε

$$\mu_{r-1} - \mu_r \le \varepsilon \mu_r , \tag{12}$$

де

$$\mu_r = \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x,y) - R_{k,l,r}(a,b; x, y) \right| . \tag{13}$$

Під час розв'язування тестових прикладів досягнення точності $\varepsilon = 0.003$ спостерігалося за вісім-дванадцять ітерацій (4), (5). Ця точність забезпечувала збіжність двох-трьох значущих цифр похибки чебишовського наближення раціональним виразом. При цьому точність $\varepsilon_1 = 0.003$, визначення проміжних наближень раціональним виразом, досягалась за три-чотири внутрішні ітерації (6)–(8). Якщо для $r \ge 1$ значення вагової функції $\upsilon_{r,0}(x, y)$ не змінювати — залишити рівними попереднім $\upsilon_{r-1,t}(x, y)$, то для уточнення раціонального виразу достатньо було лише двох ітерацій (6), (8).

Для отриманого наближення раціональним виразом (1) проводимо симетризуюче коригування. Визначаємо значення адитивної поправки

$$\overline{a}_0 = \left(\mu_{\max} + \mu_{\min} \right) / 2 , \tag{14}$$

де

$$\mu_{\max} = \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left(f(x, y) - R_{k,l}(a,b; x, y) \right) ,$$

$$\mu_{\min} = \min_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left(f(x, y) - R_{k,l}(a,b; x, y) \right) .$$

В результаті шукане чебишовське наближення неперервної функції $f(x, y)$ раціональним виразом (1) буде мати вигляд

$$R_{k,l}\left(a,b;\, x, y\right) = R_{k,l}(a,b;\, x, y) + \overline{a}_0 . \qquad (15)$$

Приклад. Знайдемо чебишовське наближення функції $z(x, y) = e^{-(x^2+y^2)}$ заданої в точках (x_i, y_j), $i = \overline{0,10}$, $j = \overline{0,10}$, де $x_i = -1 + 0.2i$, $y_j = -1 + 0.2\, j$, раціональним виразом $R_{2,2}(x, y)$, в якому чисельник і знаменник поліноми другого степеня за змінними *x* та *y*.

З використанням запропонованого методу при $\varepsilon = 0.003$ за сім ітерацій (4), (5) для функції $z(x, y)$ отримано раціональний вираз

$$R_{2,2}(x, y) = \frac{P_2(x, y)}{Q_2(x, y)}, \qquad (16)$$

в якому

$$P_2(x, y) = 1.007258776 - 0.115894128_{10}{}^{-8}\, x - 0.234478414_{10}{}^{-8}\, y -$$
$$-0.3393352184\, x^2 - 0.3393352234\, y^2 + 0.1445200801_{10}{}^{-9}\, xy,$$

$$Q_2\left(x, y\right) = 1 + 0.2634009507_{10}{}^{-8}\, x - 0.5167223229_{10}{}^{-8}\, y +$$
$$+0.7853630535\, x^2 + 0.7853630273\, y^2 + 0.4766678537_{10}{}^{-9}\, xy.$$

Раціональний вираз (16) з урахуванням коригуючої поправки $\overline{a}_0 = -0.00014942155$ забезпечує абсолютну похибку наближення — 0.007665. В процесі обчислення чебишовського наближення функції *z*(*x*, *y*) похибка наближення на ітераціях (5) набувала таких значень:

0.0153866457, 0.010443066, 0.009504082, 0.0085679,
0.007935789, 0.0078146481, 0.0078186119.

Поверхню похибки апроксимації раціональним виразом (16) показано на рисунку.

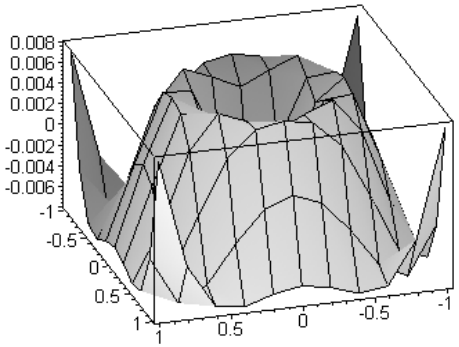

Рисунок. *Поверхня похибки апроксимації функції* $z(x, y)$ *раціональним виразом (16)*

Цей приклад взято з праці Л. В. Петрак [7], в якій для отримання чебишовського наближення функції $z(x, y)$ використано метод зведення нелінійної задачі (2) до послідовного розв'язування задач лінійного програмування. Чебишовське наближення функції $z(x, y)$ в праці [7] отримано з похибкою 0.007666 за сім звертань до процедури розв'язування задачі лінійного програмування.

Висновок. Запропонований метод побудови чебишовського наближення раціональним виразом неперервних таблично-заданих функцій забезпечує можливість обчислення наближення з необхідною точністю. Метод простий для реалізації, надійний і ефективний. Результати розв'язування тестових прикладів підтверджують досить швидку збіжність запропонованого методу при наближенні раціональним виразом функцій однієї та двох змінних. Під час розв'язування тестових прикладів за цим методом збіжність двох-трьох значущих цифр похибки чебишовського наближення раціональним виразом досягалась з використанням від восьми до дванадцяти ітерацій (4), (5).

Ідея запропонованого методу допускає його використання для апроксимації раціональним виразом неперервних таблично-заданих функцій багатьох змінних.

Список використаних джерел:

1. Коллатц Л., Крабс В. Теория приближений. Чебышевские приближения и их приложения. М. : Наука, 1978. 272 с.
2. Каленчук-Порханова А. О., Вакал Л. П. Побудова найкращих рівномірних наближень функцій багатьох змінних. *Комп'ютерні засоби, мережі та системи.* 2007. № 6. С. 141–148.
3. Петрак Л. В. Приближение функций многих переменных рациональными дробями. *Программы оптимизации*. Свердловск : УНЦ АН СССР, 1975. Вып. 6. С. 130–144.
4. Malachivskyy P. S., Matviychuk Y. N., Pizyur Y. V., Malachivskyi R. P. Uniform Approximation of Functions of Two Variables. *Cybernetics and Systems Analysis.* N 3. May–June, 2017. P. 426–431.
5. Filip S.-I., Nakatsukasa Y., Trefethen L. N., Beckermann B. Rational minimax approximation via adaptive barycentric representations. URL: https://arxiv.org/-pdf/1705.10132. 2017. P. 1–29.
6. Nakatsukasa Y., Sete `O., Trefethen L. N. The AAA algorithm for rational approximation. *SIAM J. SCI. COMPUT.* 2018. Vol. 40, N 3. P. A1494–A1522.
7. Малачівський П. С., Пізюр Я. В., Малачівський Р. П. Рівномірне наближення раціональним виразом. *Комп'ютерні технології друкарства.* 2018. № 1 (39). С. 54–59.
8. Малачівський П. С., Пізюр Я. В., Малачівський Р. П. Обчислення чебишовського наближення функцій багатьох змінних. *Обчислювальні методи і системи перетворення інформації*: зб. праць V наук.-техн. конф., Львів, 4–5 жовтня 2018 р. Львів: ФМІ НАНУ, 2018. С. 35–38.
9. Калиткин Н. Н. Численные методы. М.: Наука, 1978. 512 с.

10. Малачівський П. С., Пізюр Я. В. Розв'язування задач в середовищі Maple. Львів : Видавництво «РАСТР–7». 2016. 282 с.

CHEBYSHEV APPROXIMATION BY RATIONAL EXPRESSION FUNCTIONS OF TWO VARIABLES

The method for constructing of Chebyshev approximation by rational expression for function of two variables is proposed. Idea of the method is based on constructing the boundary power-average approximation in L^p norm with $p \to \infty$. Least square method with two weight functions is used to construct of this approximation. One weight function ensures the construction of power-average approximation, and another refines parameters of rational expression by linearization scheme. Iterative refinement of weight functions values is proposed. Results of test examples solving confirm the effectivity of proposed method.

Key words: *Chebyshev approximation by rational expression, function of two variables, power-average approximation, least square method.*

Одержано 31.01.2019

УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.81-87

А. А. Матійко

Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ NTRUENCRYPT ТА NTRUCIPHER

Асиметрична система шифрування NTRUEncrypt запропонована в 1996 р. та є однією з найшвидших постквантових шифросистем. Вона включена до стандарту ANSI X9.98-2010 та є прототипом широкого класу криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів в деяких решітках. Криптографічні властивості шифросистеми NTRUEncrypt достатньо повно досліджені, а її останні модифікації представлено на поточному конкурсі NIST із стандартизації постквантових асиметричних алгоритмів шифрування, інкапсуляції ключів та цифрового підпису.

Однією з актуальних задач у галузі криптології є створення симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї конкретної задачі (наприклад, для RSA це — задача факторизації чисел). У зв'язку з цим в 2017 р. на базі NTRUEncrypt запропонована симетрична шифросистема NTRUCipher, для якої проведено попередній аналіз стійкості та запропоновано алгоритм вибору парамет-